Seventh Circuit Review

Volume 11 | Issue 2 Article 3

9-1-2016

Is the Injury Real?: The Seventh Circuit Extends Article III Standing to Data Breach Victims

Emily P. Linehan

SEVENTH CIRCUIT REVIEW Volume 11, Issue 2 Spring 2016

IS THE INJURY REAL?: THE SEVENTH CIRCUIT EXTENDS ARTICLE III STANDING TO DATA BREACH VICTIMS

EMILY P. LINEHAN*

Cite as: Emily P. Linehan, *Is the Injury Real?: The Seventh Circuit Extends Article III Standing to Data Breach Victims*, 11 SEVENTH CIRCUIT REV. 146 (2016), *at* http://www.kentlaw.iit.edu/Documents/Academic Programs/7CR/v11-2/linehan.pdf.

INTRODUCTION

Data breaches are an increasingly common occurrence and a growing social issue. Several large corporations were hit with, or settled, large lawsuits related to data breaches, including Home Depot and Lamps Plus, Inc., in March 2016 alone. On March 8, 2016, Home Depot agreed to settle consumers' class action claims from a 2014 data breach for $13 million, in addition to funding identity protection services and implementing new data security measures.[1] Lamps Plus, Inc., was sued on March 29 for failure to protect the information of an estimated 1,300 workers following a recent target by hackers who

* J.D. candidate, May 2017, Chicago-Kent College of Law, Illinois Institute of Technology; M.A., Russian, East European, and Eurasian Studies, University of Texas at Austin, 2010; M.P.Aff., Public Affairs, University of Texas at Austin, 2010; B.A., Slavic Studies, Brown University, 2007.

[1] Allison Grande, *Home Depot to Pay $13M to End Consumers' Breach Claims*, LAW360 (April 16, 2016), http://www.law360.com/classaction/articles/768679?nl_pk=4123bead-428e-49d0-89dbace96bab2b1c&utm_source=newsletter&utm_medium=email&utm_campaign=classaction.

allegedly stole employee IRS information.[2] As of April 26, 2016, there have been 315 data breaches in the United States, affecting over 11.3 million records.[3]

In July 2015, the U.S. Court of Appeals for the Seventh Circuit addressed Article III standing of consumers who were harmed by a data breach.[4] In that case, customers brought a lawsuit against Neiman Marcus in the U.S. District Court for the Northern District of Illinois, alleging present injuries and increased risk of future harm following a 2013 data breach by hackers.[5] Plaintiffs alleged present injuries including loss of time and money related to resolving fraudulent charges and protecting against future risks, financial losses for purchases plaintiffs would not have otherwise made, and loss of control over private information.[6]

The district court held that the Plaintiffs did not adequately allege injury sufficient to establish Article III standing and granted Defendant's motion to dismiss for lack of standing.[7] While the district court found that the threat of future harm was imminent, the injuries inflicted by unauthorized credit card charges did not "qualify as 'concrete' injuries."[8] The complaint did not contain allegations regarding the costs incurred to mitigate the risk of future fraudulent charges, and the court noted that the general responses to a fraudulent charge, including issuance of a new credit card and possibly a period

[2] Kurt Orzeck, *Lamps Plus Hit With Employee Class Action Data Breach*, LAW360, (April 28, 2016), http://www.law360.com/classaction/articles/777931?nl_pk=4123bead-428e-49d0-89db-ace96bab2b1c&utm_source=newsletter&utm_medium=email&utm_campaign=classaction.

[3] *Data Breach Reports*, IDENTITY THEFT RESOURCE CENTER, at 4 (May 24, 2016), http://www.idtheftcenter.org/images/breach/DataBreachReports_2016.pdf.

[4] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

[5] Remijas v. Neiman Marcus Grp., LLC, No. 14 C 1735, 2014 WL 4627893, at *1 (N.D. Ill. Sept. 16, 2014), *rev'd and remanded*, 794 F.3d 688 (7th Cir. 2015).

[6] *Id.*

[7] *Id.* at *1, *5.

[8] *Id.* at *3.

of time where one has to wait for the new card, are *de minimis* injuries and ultimately insufficient to confer standing.[9]

On appeal, the Seventh Circuit reversed the district court's decision.[10] The Seventh Circuit considered the injuries Plaintiffs alleged and found that the Supreme Court's holding in *Clapper* did not "foreclose any use whatsoever of future injuries to support Article III standing."[11] Citing to a district court case with similar facts where the court found Article III standing,[12] the *Remijas* court held that injuries associated with resolving fraudulent charges and protecting oneself against identity theft were sufficient to satisfy the injury in fact requirement for Article III standing.[13] Thus, the Seventh Circuit held that the Plaintiffs' alleged injuries were sufficient to establish standing.[14]

Part I of this article discusses data breaches and their costs to society. Part II provides a summary of Article III standing doctrine at the Supreme Court more generally and at the federal appellate court level in cases involving data breaches. Part III reviews the factual and procedural context of *Remijas v. Neiman Marcus Group, LLC*, as well as the district court and Seventh Circuit holdings. Finally, Part IV argues that the Seventh Circuit's finding of Article III standing is proper and consistent with approaches both by the Supreme Court and those adopted by other federal courts of appeal.

WHAT IS A DATA BREACH?

According to the Congressional Research Service, "[a] data security breach occurs when there is a loss or theft of, or unauthorized access to, sensitive personally identifiable information that could result in the potential compromise of the confidentiality or integrity of

[9] *Id.* at *4.
[10] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015).
[11] *Id.* at 693.
[12] *Id.*
[13] *Id.* at 696.
[14] *Id.* at 697.

data."[15] Data breach causes include: "computer hacking, malware, payment card fraud, employee insider breach, physical loss of non-electronic records and portable devices, and inadvertent exposure of confidential data on websites or in e-mail."[16] The most frequent cause of data breaches is malicious or criminal attack, accounting for 47% of data breaches globally in FY 2015.[17]

Data breach costs also continue to increase.[18] According to the Ponemon Institute, a research center dedicated to privacy and data protection, the average per capita cost of data breaches in the United States in FY 2015 was $217, the highest in the world, which was an increase from $207 in FY 2014 and $188 in FY 2013.[19] The average total organizational cost of data breaches in FY 2015 was $6.5 million, an increase of over $1 million since FY 2013.[20] The Institute calculates data breach costs from both direct and indirect expenses. "Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates."[21]

In 2013, the House Subcommittee on Commerce, Manufacturing, and Trade held a hearing on data breaches, entitled "Reporting Data

[15] GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS 2 (2012), https://www.fas.org/sgp/crs/misc/R42475.pdf.

[16] *Id.*

[17] *2015 Cost of Data Breach Study: Global Analysis*, PONEMON INST., 10 (May 2015). Malicious and criminal attacks account for negligent insiders, individuals who cause a breach because of carelessness, and malicious attacks caused by hackers or criminal insiders, attacks include malware infections, criminal insiders, phishing/social engineering, and SQL injection. *Id.*

[18] *Id*. at 10.

[19] *Id*. at 2–5.

[20] *Id*. at 7.

[21] *Id*. at 4.

Breaches: Is Federal Legislation Needed to Protect Consumers?"[22] During the hearing, Representatives heard about data breach trends and the need for federal legislation to protect consumers.[23] There currently exists a patchwork of state laws with no federally mandated notification regime, costing businesses more than an estimated $100 billion to comply.[24]

Given the costs and frequency of data breaches, millions of Americans are at risk of having their personal information stolen. The question becomes, once a person's personal information is compromised in a data breach, does the victim have any legal recourse? Varying judicial interpretation of Article III Section 2 Clause 1 of the U.S. Constitution provides an unclear answer to this question, as without Article III standing, data breach victims cannot have their claims heard in federal court.

ARTICLE III STANDING

Article III Section 2 Clause 1 outlines the jurisdiction of U.S. courts.[25] Article III's case-or-controversy doctrines, including standing, mootness, ripeness, and political question, concern "the constitutional and prudential limits to the powers of an unelected, unrepresentative judiciary in our kind of government."[26] The Supreme Court has set forth that Article III standing is arguably the "most important" of the case-or-controversy doctrines.[27] "[S]tanding is an essential and unchanging part of the case-or-controversy requirement

[22] Press Release, The Energy and Commerce Committee, Subcommittee Explores State of Data Breaches in United States (July, 18 2013), https://energycommerce.house.gov/news-center/press-releases/subcommittee-explores-state-data-breaches-united-states.

[23] *Id*.

[24] *Id*.

[25] U.S. CONST. art. III.

[26] Allen v. Wright, 468 U.S. 737, 750 (1984) (quoting Vander Jagt v. O'Neill, 699 F.2d 1166, 1178–79 (1983) (Bork, J., concurring)).

[27] *Id*.

of Article III."[28] The Court has always required that a litigant have "standing", which "subsumes a blend of constitutional requirements and prudential considerations."[29] Until a court determines that a litigant has standing, "the court cannot proceed at all in any cause."[30] For example, federal courts do not have jurisdiction to declare a statute void unless matters before them involve "litigants in actual controversies."[31]

The Supreme Court has established that in order to find that the "irreducible constitutional minimum of standing" has been met, the plaintiff must prove the three elements.[32] The first element, injury, requires that the plaintiff have suffered "injury in fact", which is "an invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) "actual or imminent, not 'conjectural' or 'hypothetical.'"[33] The second element, causation, requires a causal connection between the injury and the "conduct complained of."[34] The third element, redressability, requires that it must be likely, and not just speculative, that the court can redress the injury.[35] The burden is on the party invoking jurisdiction to establish the three elements.[36]

While the Court has not yet addressed Article III standing in connection to a data breach, several recent cases have had and will have an impact on current and future data breach cases. In *Clapper v. Amnesty International USA*, the Court found that plaintiffs lacked standing in a case involving the federal government's wiretapping

[28] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

[29] Valley Forge Christian Coll. v. Ams. United for Separation of Church and State, Inc., 454 U.S. 464, 471 (1982).

[30] Steel Co. v. Citizens for a Better Environment, 523 U.S. 83, 94 (1998) (quoting Ex parte McCardle, 74 U.S. (7 Wall.) 506, 514 (1868)).

[31] Liverpool, N.Y. & P.S.S. Co. v. Emigration Comm'rs, 113 U.S. 33, 39 (1885).

[32] *Lujan*, 504 U.S. at 560–61; *see also* Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 179 (2000).

[33] *Lujan*, 504 U.S. at 560.

[34] *Id*.

[35] *Id*. at 561.

[36] *Id*.

program.[37] The Court held that "threatened injury must be certainly impending" in order to satisfy the injury in fact requirement.[38] Most recently, in *Spokeo, Inc. v. Robins*, the Court held that the Ninth Circuit had not properly analyzed the concreteness of a consumer's injury, one of the prongs of the injury in fact requirement,[39] and otherwise urged that "bare procedural violation(s)" are likely not enough to constitute injury in fact.[40] At the federal appellate court level, data privacy, an implicit concern involved in assessing injuries from a data breach, is currently up before the Sixth Circuit in a case involving inaccurate information a credit reporting agency released to a consumer's potential employer.[41]

The following sections will detail Supreme Court precedent on Article III standing more generally followed by Article III standing in lower court cases involving data breaches. The section on Supreme Court precedent includes an analysis of *Spokeo*, which, though it was decided after *Remijas*, did not substantively alter long-standing principles of Article III standing,[42] and creates no conflict with the Seventh Circuit's analysis and holding in *Remijas*.

A. Article III Standing and Supreme Court Precedent

In *Lujan v. Defenders of Wildlife*, the Supreme Court held that the "irreducible constitutional minimum of standing" contains the following three elements: (1) injury in fact, which is the invasion of a legally protected interest which is both concrete and particularized and actual or imminent; (2) "a causal connection between the injury and the conduct complained of"; and (3) likelihood that the injury can be

[37] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013).

[38] *Id*. at 1147.

[39] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016).

[40] *Id*. at 1544.

[41] *See* Smith v. LexisNexis Screening Solutions, Inc., 76 F. Supp. 3d 651 (E.D. Mich. 2014), *appeal docketed*, No. 15-2330 (6th Cir. Nov. 2, 2015).

[42] *See, e.g.*, Order Granting Final Approval of Class Action Settlement at 2 n.1, Chapman v. Dowman, Heintz, Boscia & Vician, P.C., No. 2:15-CV-120 JD, 2016 WL 3247872 (N.D. Ind. Dec. 29, 2015), at *1 n.1.

redressed through a favorable decision.[43] For the purposes of establishing standing at the pleading stage, "general factual allegations of injury resulting from the defendant's conduct may suffice."[44] The plaintiff bears the burden of proof, and "each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof."[45]

Plaintiffs in *Lujan* were wildlife conservation and environmental organizations who sued the Secretary of the Interior and requested the following: first, a declaratory judgment that an agency regulation was in error as to its geographic scope, and second, an injunction requiring that a new regulation be promulgated.[46] While the district court granted the Secretary's motion to dismiss for lack of standing, the Eighth Circuit reversed and remanded, holding that plaintiffs had adequately pled injury in fact.[47]

Ultimately, the Supreme Court reversed the Eighth Circuit and held that plaintiffs had not sufficiently alleged an injury as a result of the defendant's actions.[48] Justice Scalia, writing for the majority, urged a higher threshold for standing and invalidated a congressional grant of standing for the first time because of the absence of sufficient injury in fact.[49] Injury in fact required more than a cognizable interest; it required that the parties seeking review have themselves been injured.[50] Plaintiffs argued that they had suffered injury in fact because agency-funded projects would eliminate endangered species in locations plaintiffs intended to visit, but these arguments "[did] not support a finding of 'actual or imminent' injury that [Supreme Court]

[43] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

[44] *Id.* at 561.

[45] *Id.*

[46] *Id.* at 558–59.

[47] Defenders of Wildlife, Friends of Animals & Their Environment v. Hodel, 851 F.2d 1035, 1041 (8th Cir. 1988)

[48] *Lujan*, 504 U.S. at 562.

[49] Seth F. Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 749-50 (2016).

[50] *Lujan*, 504 U.S. at 562–63.

cases require."[51] The Court held that standing requires "a factual showing of perceptible harm."[52] *Lujan* emphasized that concreteness is essential to the injury in fact requirement.[53]

Shortly after *Lujan* was decided, the Supreme Court ruled unanimously against the government in a case involving the IRS's allegedly illicit acquisition of tapes involving conversations between the Church of Scientology members and its attorneys.[54] In that case, the Los Angeles County Court Clerk released the tapes to the IRS, which the IRS had requested in connection with an investigation into the tax returns of L. Ron Hubbard, the founder of the Church of Scientology.[55] Given the physical delivery of the tapes, the United States argued that the Church had "lost its claim to avoid a threatened injury in fact."[56] The Court held that the taxpayer was still suffering injury as a result of the Government's possession of the tapes in the form of an "affront to the taxpayer's privacy."[57] Though the case was centered on the question of mootness under Article III, not standing, the case reveals that the Court found injury in fact where personal information is concerned. This suggests that conferring standing for a breach in which such information is stolen and subject to fraud, when there is a strong possibility for future fraudulent conduct, is not contrary to the Court's holding.

More recently, in *Clapper v. Amnesty International USA*, the Court held that attorneys and human rights, labor, legal, and media organizations did not have standing because they alleged future harm that was not "certainly impending."[58] The plaintiffs challenged the Foreign Intelligence Surveillance Act (FISA) Amendments Act of

[51] *Id.* at 564.

[52] *Id.* at 566.

[53] *Id*. at 578.

[54] Church of Scientology of Cal. v. U.S., 506 U.S. 9, 10 (1992).

[55] *Id.*

[56] Kreimer, *supra* note 49, at 760 (citing *Church of Scientology*, 506 U.S. at 10).

[57] *Church of Scientology*, 506 U.S. at 13.

[58] 133 S. Ct. 1138, 1143 (2013).

2008, 50 U.S.C. § 1881(a), which permitted the Government to target and surveil communications of non-U.S. citizens abroad.[59] Plaintiffs regularly communicated with colleagues and clients abroad, and they alleged that the new law forced them to undertake costly measures to protect the confidentiality of their communications.[60] The Court held that plaintiffs suffered self-inflicted injuries and "subjective fear of surveillance," neither of which gave rise to standing.[61] In its analysis, the Court also rejected an alternative argument that present measures taken to prevent future harm could constitute an injury sufficient to confer standing.[62]

The Court focused on an injury's imminence, conceding that it was "a somewhat elastic concept," but that in order to satisfy the element of imminence, the injury must be "certainly impending."[63] Allegations of possible future injury are not sufficient to be considered "certainly impending."[64] The Court held that plaintiffs rested their theory of standing on a "highly attenuated chain of possibilities," including: (1) the Government would imminently target their communications; (2) the Government would invoke its surveillance authority under § 1881a; (3) Article III judges would approve the Government's surveillance plan; (4) the Government would intercept communications from respondents' contacts; and (5) the Government would intercept respondents' communications.[65] This "speculative chain of possibilities" did not establish that injury based on future surveillance was "certainly impending" or fairly traceable to section 1881(a).[66]

[59] *Id.* at 1144; 50 USCA § 1881a.

[60] *Id.* at 1144-45.

[61] *Id.* 1152–53.

[62] *Id.* at 1143.

[63] *Id.* at 1147 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

[64] *Id.* (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990).

[65] *Id.* at 1148–50.

[66] *Id.* at 1150.

Plaintiffs also argued in the alternative that they were suffering present injuries by taking measures to avoid section 1881(a) surveillance.[67] The Court rejected this theory of standing as well, holding that the Second Circuit had improperly "water[ed] down the fundamental requirements of Article III" by allowing that the present costs incurred by taking protective measures were sufficient for standing as long as they were not "fanciful, paranoid, or otherwise unreasonable."[68]

Justice Breyer wrote for the dissent and argued that the harm alleged was not "speculative" and was "as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen."[69] Given that all agreed that interception of the phone calls or emails would qualify as "concrete and particularized" injury, and a favorable judgment by the Court would redress the injury by declaring the statute unconstitutional, the principle issue was whether the interception of the communications was an injury that was "actual or imminent."[70] The dissent argued that the case law suggested that the Constitution did not require that injury be an absolute certainty, but rather a "reasonable" or "high probability."[71] Notwithstanding their disagreement, both the majority and dissent conceded that an actual interception would constitute an injury sufficient to confer standing.

Though the Court did not find injury in fact in *Clapper*, the Court has ruled in favor of plaintiffs whose "legitimate expectations of privacy" have been violated.[72] Relevant cases involving intangible acquisition of private information have created a potential Fourth Amendment violation, including in cases involving thermal imaging,

[67] *Id.*

[68] *Id.* at 1151.

[69] *Id.* at 1155 (Breyer, J., dissenting).

[70] *Id.* at 1155–56.

[71] *Id.* at 1165.

[72] Kreimer, *supra* note 49, at 758 (citing Katz v. United States, 389 U.S. 347, 353 (1967) (ruling that the "presence or absence of a physical intrusion" cannot be a meaningful distinction in Fourth Amendment cases)).

analysis of blood and urine samples, analysis of information in cell phones seized upon arrest, and GPS monitoring.[73] Intangible intrusions on privacy are enough to create constitutional violations, and therefore, it is not unreasonable that the unquestioned theft of personal information in a data breach may qualify as injurious enough for the purposes of standing.

Finally, in its most recent term, the Court decided *Spokeo*, another case involving concreteness and the injury in fact requirement.[74] In *Spokeo*, the case before the Court involved an action brought by a consumer under the Fair Credit Reporting Act ("FCRA") against a website operator for publishing an inaccurate consumer report about him. In a 6–2 decision, the Court vacated the Ninth Circuit's decision and remanded, holding that the lower court's standing analysis was incomplete and had "failed to fully appreciate the distinction between concreteness and particularization."[75] The Court expressed no opinion as to whether Robins had standing and remanded the question of the concreteness of Robins' injury to the Ninth Circuit.

Writing for the majority, Justice Alito stated that for an injury to be "concrete" it must "actually exist[,]"[76] while also noting that an injury need not be tangible to exist.[77] The Court permitted that procedural violations, such as a violation of the FCRA, might be sufficient to constitute an injury in fact, but a "bare procedural violation" such as "an incorrect zip code" would not cause concrete harm.[78] The opinion has generated headlines, with both plaintiff and defense bars claiming that the opinion was a positive one for their

[73] *Id.* at 758 (citing Kyllo v. United States, 389 U.S. 347, 353 (1967); Ferguson v. City of Charleston, 532 U.S. 67, 76 (2001); Riley v. California, 134 S. Ct. 2473, 2489–90 n.1 (2014)).

[74] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016).

[75] *Id.* at 1550.

[76] *Id.* at 1548.

[77] *Id.* at 1549.

[78] *Id.* at 1550.

respective sides of the aisle.[79] Regardless of who benefited from *Spokeo*, it does not create conflict for the *Remijas* holding, in which the court adequately addressed both prongs of injury in fact, as the discussion *infra* will demonstrate. While *Spokeo* does not provide any additional guidance to cases with similar facts to *Remijas*, the cases discussed in the next section, which deal with data breaches, or data privacy, provide more insight into the correctness of the *Remijas* court's ruling.

B. Article III Standing and Data Breaches

Though no federal appellate court prior to the *Remijas* court has ruled on any data breach cases which specifically involve fraudulent charges, courts have dealt with data breaches and varying allegations of injury. No case other than *Remijas* was decided after *Clapper*, however, and therefore, only the Seventh Circuit had occasion to interpret *Clapper* in a case involving a data breach. Other courts primarily relied on the Supreme Court's enunciation of Article III standing in *Lujan.*

In 2012, the Eleventh Circuit addressed alleged injuries from identity theft that resulted from a data breach in a case of first impression.[80] The plaintiffs filed suit when a health care services corporation was burgled and two laptops containing sensitive and personal customer information was compromised.[81] *Resnick v. Avmed, Inc.* was decided before *Clapper*, thus the court relied on *Lujan*, in which the Supreme Court held that "general factual allegations of injury resulting from the defendant's conduct may suffice" to establish standing.[82] Under that standard, the court quickly concluded that

[79] Allison Grande, *Spokeo Ruling Helps Both Sides of the Privacy Bar, Attys Say*, LAW360 (May 25, 2016), http://www.law360.com/articles/800443/spokeo-ruling-helps-both-sides-of-privacy-bar-attys-say.

[80] Resnick v. Avmed Inc., 693 F.3d 1317, 1323 (11th Cir. 2012).

[81] *Id.* at 1322.

[82] *Id.* at 1323 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992)).

allegations of actual identity theft and monetary damages were injury in fact under the law.[83] Though the Seventh Circuit did not cite *Resnick* in *Remijas*,[84] the *Resnick* court's conclusion that identity theft and monetary damages constituted injury in fact lends strength to the idea that a data breach that results in fraudulent charges has similarly pled an increased likelihood of identity theft and therefore injury in fact.

In data breach cases before the Seventh and Ninth Circuits, both courts held that plaintiffs had sufficiently pled injury in fact to satisfy Article III standing. In *Pisciotta v. Old National Bancorp*, plaintiffs alleged that hackers who gained access to bank customers' personal information had caused injury in fact. The Seventh Circuit relied on the reasoning of sister circuit courts[85] and held that injury in fact "can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm[,]" even if plaintiffs provide no proof of data misuse.[86]

In *Krottner v. Starbucks Corp.*, the Ninth Circuit relied on slightly different reasoning than the Seventh Circuit and held that if a plaintiff faces a credible threat of harm that is real and immediate, and not conjectural or hypothetical, then the plaintiff has met the injury in fact requirement for Article III standing.[87] To formulate this test, the court relied on Ninth Circuit precedent and a Supreme Court case, *City of Los Angeles v. Lyons*.[88] In *Krottner*, a laptop was stolen from Starbucks that contained the unencrypted personal information of 97,000 employees.[89] Following the theft, one of the plaintiffs was

[83] *Id*.

[84] *See generally* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

[85] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 n.3 (7th Cir. 2007) (citing to opinions in the Second, Sixth, Ninth and Fourth Circuits, in which the courts held that threats of future harm conferred standing).

[86] *Id*.

[87] Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

[88] *Id*. (citing City of Los Angeles v. Lyons, 461 U.S. 95, 102 (1983); Cent. Delta Water Agency v. United States, 306 F.3d 947, 950 (9th Cir. 2002)).

[89] *Krottner*, 628 F.3d at 1141.

notified by his bank that someone had tried to open an account in his name.[90] Plaintiffs enrolled in free credit monitoring services and spent extra time monitoring their accounts.[91] Given these facts, the court held that the theft created "real and immediate harm."[92]

In contrast, the Third Circuit ruled that data breach victims had not successfully pled injuries sufficient to find Article III standing.[93] In *Reilly v. Ceridian Corp.*, plaintiffs were employees of companies which were customers of a payroll processing firm (Ceridian Corporation).[94] A hacker infiltrated the company's payment system and "*potentially* gained access to personal and financial information" of the company's customer businesses.[95] Though there was a security breach, the plaintiffs did not provide the court any proof that the hacker "read, copied, or understood the data," and the court held that the allegations of future injury were therefore too hypothetical.[96] The injuries alleged were even more speculative than those in *Lujan*, which the Supreme Court held were insufficient to confer standing.[97] The court also distinguished the facts from those in *Krottner* and *Pisciotta*, finding that those cases involved "harms [that] were significantly more 'imminent' and 'certainly impending' than the alleged harm here."[98]

With *Remijas*, the Seventh Circuit relied on more recent Supreme Court precedent, while adhering to the principles the cases above set out regarding the injury in fact requirement. Per the holdings above, in data breach cases, evidence that hackers have misused information clearly makes a stronger case for conferring Article III standing.

[90] *Id*.
[91] *Id*.
[92] *Id*. at 1143.
[93] Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011).
[94] *Id*. at 40.
[95] *Id*. (emphasis added).
[96] *Id*.
[97] *Id*. at 42.
[98] *Id*. at 44.

REMIJAS V. NEIMAN MARCUS

A. Factual Background

Neiman Marcus, a luxury department store, was attacked by hackers who stole customers' credit card numbers during the holiday season in 2013.[99] In December 2013, Neiman Marcus determined that as a result of the hack, some customers had fraudulent charges on their credit cards.[100] Once Neiman Marcus learned of the fraudulent charges, the company investigated and found potential malware in its computer systems, which had attempted to collect customer card data between July 16, 2013 and October 30, 2013.[101] The company announced on January 10, 2014, that it had determined that approximately 350,000 credit cards had been exposed to the hackers' malware.[102] Neiman Marcus then publicly disclosed the data breach and revealed that of those 350,000, 9200 cards were known to have been used fraudulently.[103] Not only were credit card numbers exposed, but also social security numbers and birth dates.[104] Neiman Marcus was not the only company to suffer security breaches during that holiday season.[105]

Neiman Marcus notified its customers who had shopped at its stores between January 2013 and January 2014 and offered them "one year of free credit monitoring and identify theft protection."[106] Following this announcement, on February 4, 2014, Michael Kingston,

[99] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 689 (7th Cir. 2015).

[100] *Id.* at 689–90.

[101] *Id.* at 690.

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] Target and Michael's were also targeted. *See* Christopher Budd, *Information about recent retail data breaches in the United States: an FAQ*, TREND MICRO: SIMPLY SECURITY, (last visited April 19, 2016), http://blog.trendmicro.com/information-recent-retail-data-breaches-united-states-faq/.

[106] *Remijas*, 794 F.3d at 690.

Senior Vice President and Chief Information Officer, testified before the United States Senate Judiciary Committee, representing that the information that appeared to have been compromised was credit card information, with no indication that social security numbers or other private information had been compromised.[107] Several lawsuits were filed, and these were consolidated into the complaint that gave rise to this case, *Remijas v. Neiman Marcus*.

In the complaint, Hilary Remijas alleged that she made purchases at the Neiman Marcus in Oak Brook, Illinois, in August 2013 and December 2013.[108] Melissa Frank, another named plaintiff, alleged that she used a joint debit card to make purchases at the Neiman Marcus in Long Island, New York in December 2013.[109] Frank further alleged that she was a target of a scam through her cell phone and that her husband had received a letter about the breach from Neiman Marcus.[110] The final named plaintiff, Joanne Kao, alleged that she made purchases on ten separate occasions over the course of 2013 at a Neiman Marcus store location in San Francisco, and that she received notifications about the breach from both Neiman Marcus and her bank.[111]

B. Procedural Background

Hilary Remijas joined several other plaintiffs to file a class-action complaint against Neiman Marcus on June 2, 2014, seeking to represent themselves and the 350,000 other customers whose personal information may have been hacked.[112] The complaint relies on theories for relief that include "negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of

[107] *Id.*

[108] *Id.* at 691.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.* at 690; Remijas v. Neiman Marcus Group, LLC, No. 14 C 1735, 2014 WL 4627893, at *1 (N.D. Ill. Sept. 16, 2014).

privacy, and violation of multiple state data breach laws."[113] Defendant, Neiman Marcus, moved to dismiss the complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for lack of standing and failure to state a claim.[114] The District Court granted the motion to dismiss on standing grounds.[115]

C. The District Court's Decision

District Judge Zagel analyzed the plaintiffs' alleged injuries and held that plaintiffs had failed to plead Article III standing sufficiently. He noted that Article III standing is not "a mere pleading requirement," but rather must be supported "with the manner and degree of evidence required at the successive stages of the litigation."[116] Plaintiffs alleged four principle categories of injury, and Judge Zagel was unpersuaded that any sufficiently supported Article III standing.[117]

The first principle category of injury that Plaintiffs alleged was increased risk of future harm.[118] Judge Zagel relied on three different cases where the court had previously addressed Article III standing in the context of cyber-attacks and analyzed how they interpreted the Supreme Court's recent decision in *Clapper.*[119] The courts in two previous cases, *Strautins v. Trustwave Holdings, Inc.*[120] and *In Re Barnes & Noble Pin Pad Litigation*[121] held that "the alleged increased risk of future harm was insufficient to establish standing."[122] The

[113] *Id*. at 690–91.

[114] *Id*. at 691.

[115] *Id.*

[116] Remijas v. Neiman Marcus Group, LLC, No. 14 C 1735, 2014 WL 4627893, at *1 (N.D. Ill. Sept. 16, 2014).

[117] *Id*. at *5.

[118] *Id*. at *2.

[119] *Id.*

[120] No. 12 C 09115, 2014 WL 960816 (N.D. Ill. Mar. 12, 2014).

[121] No. 12–cv–8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013).

[122] Remijas, 2014 WL 4627893, at *2.

Strautins and *Barnes & Noble* court both relied on *Clapper*, which required "certainly impending" analysis with regard to the injury in fact element of standing.[123] The *Strautins* court also argued that *Clapper* overruled previous Seventh Circuit precedent, which held that the "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[124]

In another case, the alleged increased risk of future harm was sufficient to establish Article III standing.[125] In *Moyer v. Michael Stores, Inc.*, the court found that while *Clapper* established a heightened standard for standing analysis, such a standard was only appropriate for situations that called for more rigor—namely, national security and the Constitution.[126] The court concluded that *Clapper* and *Pisciotta* could co-exist.[127]

Judge Zagel noted that while a literal reading of *Pisciotta* might lead to the conclusion that any increase in risk of future harm would be sufficient to confer Article III standing, this was an improper reading.[128] The standing threshold was therefore somewhere in the middle, requiring more than a mere increase of risk of harm, but less than *Clapper*'s heightened standard. Regarding the facts, Judge Zagel differentiated *Pisciotta* from *Strautins* and *Barnes & Noble*, as the plaintiffs' data in *Pisciotta* was actually stolen, while the data in the latter two cases was only alleged to have *possibly* been stolen.[129] Given that the data in *Pisciotta* was actually stolen, Judge Zagel argued that the *Pisciotta* court's holding satisfied the "certainly

[123] *Id.*

[124] *Id.* (citing Pisciotta v. Old Nat'l Bancorp, 499 F.2d 629, 634 (7th Cir. 2007)).

[125] Moyer v. Michael Stores, Inc., No. 14 C 561, 2014 WL 3511500 at *4–5 (N.D. Ill. July 14, 2014).

[126] *Id.*

[127] *Id.* at *2 (citing *Moyer*, 2014 WL 3511500, at *6).

[128] *Id.*

[129] *Id.* at *3.

impending" standard, while *Strautins* and *Barnes & Noble*, where data was only possible stolen, did not satisfy the standard.[130]

Applying this understanding to *Remijas*, Judge Zagel held that the majority of Plaintiffs were only alleging that their data may have been stolen, which made the case more like *Strautins* and *Barnes & Noble*.[131] Though Plaintiffs also alleged that 9200 of the 350,000 customers had fraudulent charges appear on their credit cards, Judge Zagel held that this was not enough to prove an injury to confer standing.[132] Judge Zagel determined that the fraudulent charges led to several inferences: (1) there was injury in fact, which could be inferred from the fact that 9200 customers had their data stolen, and (2) there was injury in fact that was "certainly impending" for the remaining customers among the 350,000, who might experience fraudulent charges in the future.[133] Relying on *Clapper*, neither inference demonstrated injury that was "concrete, particularized, and, if not actual, at least imminent."[134] While Judge Zagel found that potential future fraudulent charges were sufficiently "imminent" for standing, the injuries were not sufficiently concrete.[135] Plaintiffs who suffered fraudulent charges did not allege that they were unreimbursed, and therefore the charges for which plaintiffs were not financially responsible did not qualify as "concrete" injuries.[136]

Additionally, Judge Zagel was not persuaded that the customers were at a "certainly impending risk of identity theft." The fact that 9200 Plaintiffs had incurred fraudulent charges on their credit cards only supported an inference that their credit card information was stolen.[137] While this placed the remaining Plaintiffs at a "certainly impending" risk of incurring fraudulent charges themselves, Judge

[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.*

Zagel held that this did not render Plaintiffs at "certainly impending" risk of suffering future identity theft.[138]

Judge Zagel dispensed with the Plaintiffs' other alleged injuries, finding none of them to be sufficient to confer standing.[139] Plaintiffs alleged that time and money allegedly spent to mitigate risk of future fraudulent charges and identity theft constituted injury that conferred standing.[140] Citing *Moyer*, Judge Zagel noted that the costs of guarding against a risked future injury only confer standing when the underlying injury the plaintiff is trying to avoid "is itself a cognizable Article III injury."[141] Judge Zagel argued that the allegations regarding what was done to mitigate future risk were insufficient, and the steps normally taken when fraudulent charges appear (reimbursement and new card issuance) don't rise above a *de minimis* injury.[142] Further, Judge Zagel reiterated that the complaint did not adequately allege the risk of identity theft that was sufficiently imminent, and therefore, the efforts to mitigate are not cognizable Article III injuries.[143]

Plaintiffs also claimed that they suffered injury in that they paid a premium purchase price for retail goods at the Defendant's stores, a portion of which the Defendant was required to use for data breach protection services.[144] In other words, the Plaintiffs' theory was because they overpaid, they suffered financial injuries.[145] Judge Zagel held that Plaintiffs relied on case law that found injury when the value-reducing injury was "intrinsic to the product at issue."[146] Here,

[138] *Id.* at *3–4.

[139] *Id.* at *4–5.

[140] *Id.* at *4.

[141] *Id.* (citing Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *4 n.1 (N.D. Ill. July 14, 2014)).

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.*

however, "the deficiency complained of is extrinsic to the product" and therefore is a meaningless theory of injury.[147]

Finally, Judge Zagel addressed Plaintiffs' alleged injury due to "loss of control over and value of their private information."[148] Citing *Barnes & Noble*, Judge Zagel held that the injury as pled was not sufficiently concrete.[149]

D. The Seventh Circuit's Decision

Chief Judge Wood, joined by Judge Kanne and Judge Tinder, reversed the District Court's decision, finding that the plaintiffs had plausibly alleged Article III standing.[150] The case was reviewed *de novo*, consistent with the court's precedent.[151] The court analyzed both the requirements of Article III standing and, more briefly, Neiman Marcus's argument that the complaint should be dismissed for failure to state a claim.[152]

The court addressed the Plaintiffs' imminent and actual injuries as pled.[153] The two imminent injuries included: first, an increased risk of future fraudulent charges and second, greater susceptibility to identity theft. The four actual injuries included:

> 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known

[147] *Id*. at *5.

[148] *Id*.

[149] *Id*. at *5 (citing *In re* Barnes & Noble Pin Pad Litigation, No. 12–cv–8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013) (finding no actual injury where plaintiffs did not allege that their personal information was sold or that the plaintiffs themselves could have sold it)).

[150] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015).

[151] *Id.* at 691 (citing Reid L. v. Ill. State Bd. of Educ., 358 F.3d 511, 515 (7th Cir. 2004)).

[152] *Id.* at 692.

[153] *Id*.

> of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information.[154]

With regard to Plaintiffs' four alleged injuries, Chief Judge Wood noted that the allegations went "far beyond" allegations in *Spokeo*, therefore differentiating the injuries alleged here from the injuries alleged to have resulted from the publication of inaccurate information on a website.[155]

The Seventh Circuit, relying on Supreme Court precedent in *Clapper*, noted that Article III standing requires that the injury have already occurred or be "certainly impending."[156] Chief Judge Wood summarized the injuries alleged: that each Plaintiff's personal data had been stolen; that, of the 350,000 customers, 9200 incurred fraudulent charges and experienced harm; that the 9200 suffered the "aggravation and loss of value of the time needed to set things straight"; and that the remaining customers suffered a concrete risk of similar harm.[157] Chief Judge Wood identified the question as whether one of the following conditions was met under *Clapper*: either the harm had already occurred, or it was "certainly impending."[158]

Disagreeing with the district court's interpretation of *Clapper*'s precedent, Chief Judge Wood held that *Clapper* did not "foreclose any use whatsoever of future injuries to support Article III standing."[159] With *Clapper*, the Supreme Court held that the plaintiff human rights organizations did not have standing to challenge the Foreign Intelligence Surveillance Act because plaintiffs only suspected that interceptions of their communications with suspected terrorists *might have occurred*, not that any such interceptions did occur.[160] These suspicions were too speculative for the purposes of establishing Article

[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.* at 693.
[160] *Id.*

III standing.[161] Chief Judge Wood went on to quote *Clapper*, clarifying that plaintiffs are not charged with demonstrating that they are "literally certain that the harms they identify will come about . . . [and] we have found standing based on a 'substantial risk' that harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[162]

Chief Judge Wood cited to another district court that found that substantial risk sufficed for Article III standing in a data breach case in which that court held that "the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real."[163] Unlike in *Clapper*, where plaintiffs could only speculate as to whether their communications had been intercepted, here the plaintiffs' information was stolen.[164] Chief Judge Wood argued that Plaintiffs here should not have to wait for hackers to act on their personal information, either by running up fraudulent charges on their credit cards or by committing identity theft.[165]

Chief Judge Wood further argued that the very fact of the hack made it plausible to infer that Plaintiffs had shown a substantial risk of harm, as it was reasonably assumed that the purpose of the hack was "to make fraudulent charges or assume those consumers' identities."[166]

THE SEVENTH CIRCUIT'S FINDING OF ARTICLE III STANDING COMPORTS WITH PRECEDENT AND CONSISTENCY

The Seventh Circuit rested its opinion on a clear distinction between the facts in *Remijas* and *Clapper*. In *Clapper,* the Supreme Court held that possible future injuries did not satisfy the "certainly

[161] *Id.*

[162] *Id.* (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013)).

[163] *Id.* (citing *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. Sept. 4, 2014)).

[164] *Id.*

[165] *Id.*

[166] *Id.*

impending" standard required to insure that injuries are not too speculative for Article III purposes.[167] The Seventh Circuit held that the district court had both misapplied *Clapper* and improperly read out the idea that "substantial risk" of future injury was also available to support standing.[168] Indeed, just one year after *Clapper*, the Supreme Court held that an allegation of future injury could suffice if the threatened injury was "certainly impending" *or* there was a "substantial risk" that harm would occur in the future.[169] Therefore, there is no question that the substantial risk standard that the Seventh Circuit used to assess injury in fact as alleged in *Remijas* was appropriate.

While multiple federal appellate courts have addressed data breaches, including the Eleventh, Ninth, Third, and First Circuits, only the Seventh Circuit has applied *Clapper* in a data breach case. The Seventh Circuit recently applied its own precedent in *Lewert v. P.F. Chang's China Bistro, Inc.*, a case in which the plaintiffs alleged future and present injuries following a computer system breach in which consumer credit card information was stolen.[170] The Seventh Circuit held that increased risk of fraudulent charges and identity theft were plausible future injuries because the data had already been stolen.[171] The plaintiffs also successfully alleged present injuries, including fraudulent charges, and time and effort mitigating charges and preventing future fraud.[172]

In a recent data breach case at the district court level, the District Court of Maryland argued that courts generally find that the increased risk of identity theft without evidence of actual theft of personal

[167] *Clapper*, 133 S. Ct. at 1147.

[168] *Remijas*, 794 F.3d at 693.

[169] Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) (citing *Clapper*, 133 S. Ct. at 1147, 1150 n.5).

[170] No. 14–3700, 2016 WL 1459226 at *1 (7th Cir. 2016).

[171] *Id.* at *3.

[172] *Id.*

information does not confer standing.[173] The court cited to *Remijas* and *Krottner* as examples of cases in which the facts supported standing, because "allegations included either actual examples of the use of the fruits of the data breach for identity theft, even if involving victims other than the named plaintiffs, or a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud."[174] The majority of district courts have found no standing in the absence of specific incidents or evidence of intent to use stolen information.[175] *Remijas* therefore fits well within the majority approach.

Future implications of the above-discussed approach are great as data breaches continue to occur, and more lawsuits follow. In March 2016, a student filed a class action lawsuit against the University of Central Florida, alleging negligence that allowed hackers to store personal information of more than 60,000 students and faculty.[176] Had the plaintiffs alleged identity theft, per Eleventh Circuit precedent, the plaintiffs could have successfully alleged Article III standing.[177] This case was voluntarily dismissed,[178] but such cases are likely to continue to arise, as personally identifiable information is increasingly stored online by schools, employers, hospitals, and other goods and services providers with varying degrees of protection.

Remijas also fits well within *Spokeo*, which reiterated that concreteness is an essential element of the injury in fact requirement. *Spokeo* has raised numerous questions for litigants regarding how statutorily created harms interact with Article III standing, but the Court did not disturb precedent regarding concreteness. Per *Spokeo*, an

[173] Khan v. Children's Nat'l Health System, No. TDC-15-2125, 2016 WL 2946165, *9 (D. Md. May 19, 2016).

[174] *Id.* at *4.

[175] In re Zappos.com, Inc., 108 F. Supp.3d 949, 955 (D. Nev. 2015) (listing post-*Clapper* cases).

[176] Complaint, Heller v. Univ. of Cent. Fla. Bd. of Trs., No. 6:16-cv-396, 2016 WL 887470 (M.D. Fla. Mar. 6, 2016).

[177] *See* Resnick v. Avmed Inc., 693 F.3d 1317, 1323 (11th Cir. 2012).

[178] Notice of Voluntary Dismissal Without Prejudice, Heller v. Univ. of Cent. Fla. Bd. of Trs., No. 6:16-cv-396, 2016 WL 887470 (M.D. Fla. Mar. 6, 2016).

injury need not be tangible to be concrete,[179] which is critical for data breach victims, whose injuries will generally be intangible.

Several federal appellate courts have dealt with *Spokeo* in recent decisions, scrutinizing plaintiffs' alleged harms more closely. In *Hancock v. Urban Outfitters, Inc.*, the D.C. Circuit Court of Appeals drew a distinction between bare procedural harms and harms like those suffered by data breach victims and noted that the plaintiffs had asserted only "a bare violation of the requirements of D.C. law[,]" as opposed to "any invasion of privacy, increased risk of fraud or identity theft." [180] In a case involving alleged violations of disclosure requirements of the Fair Debt Collection Practices Act, the Eleventh Circuit held that the plaintiff had satisfied Article III standing requirements, as the harms she alleged were intangible but "real."[181] These opinions make clear that *Remijas* did not overreach or overextend Article III standing and was correctly decided.

CONCLUSION

The Supreme Court has yet to rule on a case in which actual fraud has occurred in the wake of a data breach. Given the standards articulated for Article III standing, requiring that injuries be "certainly impending" and sufficiently concrete, the Seventh Circuit's recent opinion in *Remijas v. Neiman Marcus, LLC* was correctly reached. The Seventh Circuit followed Supreme Court reasoning on Article III standing to find that actual injury had been sufficiently alleged in *Remijas*. When faced with similar facts, other federal courts of appeal should adopt this approach and find that fraudulent activity following a data breach constitutes injury in fact sufficient to confer Article III standing. In cases where data breaches do not result in any known

[179] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

[180] Hancock v. Urban Outfitters, Inc., No. 14-7047, 2016 WL 3996710, at *6-7 (D.C. Cir. July 26, 2016) ("The Supreme Court's decision in *Spokeo* thus closes the door on [plaintiffs'] claim that the Stores' mere request for a zip code, standing alone, amounted to an Article III injury.")

[181] Church v. Accretive Health, Inc., No. 15-15708, 2016 WL 3611543 at *9 (11th Cir. July 6, 2016).

fraudulent activity, and where plaintiffs are unsure if the information was used at all, *Remijas* is likely to be less helpful for plaintiffs. With *Remijas*, the Seventh Circuit merely recognized that fraudulent activity makes identity theft and future fraudulent charges more likely, removing a single, but critical, barrier for plaintiffs seeking relief in court.